الوصايا العشر لحماية الكمبيوتر

حارب فيروسات الكمبيوتر بجميع أنواعها بما فيها أحصنة طروادة والسبام وفيروسات البريد الإلكترونى وغيرها بإتباع الوصاياالعشر التى نطرحها فى هذا المقال
بالرغم من أن نظام ويندوز هو أشهر أنظمة التشغيل ، وبه تعمل أغلب أجهزة الكمبيوتر فى العالم ، ولا ننكر أن العمل به أمر جيد إلا أن تلك الأجهزة التى تعمل من خلال ويندوز سهلة المهاجمة ، أى تخترقها فيروسات قد تدمر شبكة كاملة بالإضافة إلى فيروسات الإيميل التى تتكاثر وتنتشر و فيروسات أحصنة طروادة.. تلك الفيروسات التى تختبئ داخل البرامج العادية. هذا بالإضافة إلى الهاكرز أى مخترقي أجهزة الكمبيوتر .

إليك الوصايا العشر للحماية من كل هذا :

1 لا تستغن أبداً عن برامج الفيروسات وتحديثاتها

لا يكفى أن تقوم بتثبيت البرنامج (إن لم يكن لديك برنامج فيروسات.. أسرع فى الحصول علية) بل تحتاج أيضاً إلى تحديثه دائماً فالفيروسات الجديدة تظهر باستمرار وجودة البرنامج المضاد للفيروسات تتوقف على أحدث التحديثات للفيروسات .

2 لا تفتح مرفقات الرسائل الإلكترونية

تصور أن رسالة وصلت إلى بريدك وأنت تظن أنها من صديق وبها مرفق يبدو أنه شيق ، ثم قمت بالضغط عليه . ما يحدث بعد ذلك هو إصابة بريدك بفيروس ينتشر إلى كل الشخصيات فى دفتر عناوينك. تلك هي طريقة انتشار فيروسات مثل So big .F worm وحدث أن انتشرت بشكل هائل وتواجد منها ملايين النسخ قبل أن تقوم شركات البرامج المضادة للفيروسات بتحديث قاعدة بياناتها.
لا تثق عشوائياً بأي إيميل يصلك ولا تفتح أى مرفق attachment قبل التيقن من أنه مرسل من قبل شخص موثوق به وأنك أنت المقصود .

3 لا تقم بتنزيل ملف خادع

كن واعياً.. فلا توافق على طلب أى موقع يطلب منك إنزال برنامج لمشاهدة صفحة ما ، إلا إذا كان برنامج معروف مثل Flash playing أو Acrobat Reaer فقد يكون الملف مصاب بفيروس أو حصان طروادة. لا تقم بتثبيت برنامج من الويب إلا إذا كنت متيقاً من ماهية هذا البرنامج وأنك تثق بتلك الشركة صاحبة الموقع الذي ستقوم بإنزال البرنامج منه.

4 لا تتهاون مع برامج التجسس والنوافذ تلقائية الفتح

تقوم برامج التجسس بتثبيت نفسها بدون علمك عندما تقوم بإنزال برنامج مثل تطبيقات File-swapping. تلك البرامج تتبع حركاتك عبر الإنترنت وتقوم بإرسال إعلانات حسب إهتماماتك، أما النوافذ تلقائية الفتح يمكنها أيضاً أن تفسد عليك الحماية فى متصفح الإنترنت مثل فيروس Q host Trojan الذى هاجم المتصفحات بعد مشاهدة إعلان موقع ما . من حسن الحظ توجد أدوات لحمايتك من هذا العبث مثل برنامج Ad-ware و Stapzilla وتوجد بعض البرامج المضادة للفيروسات توقف برامج التجسس والنوافذ تلقائية الفتح أيضاً .

5 لا تترك سبام Spam تزعجك

سبام Spam هي رسائل البريد الإلكترونى الإعلانية التى تصل إليك وأنت لم تطلبها أصلاً . فهي رسائل مزعجة وهى المصدر الرئيسي للإصابة بالفيروسات، وبعض الأحيان تجعل جهازك نفسه يرسل سبام. وهناك برامج جيدة مضادة لسبام مثل Norton antispam و McAfee spam killer والبرنامج القوي

IHatespam.

6 لا تترك نظام التشغيل بدون تحديث مستمر

تستطيع العديد من الفيروسات الخاصة بالبريد الإلكتروني وغيرها أن تستغل الثغرات الأمنية فى برنامجك سواء نظام التشغيل ويندوز أو تطبيقات مايكروسوفت. لذلك تقوم مايكروسوفت بعرض الكثير من التحديثات التي تصلح من تلك الثغرات التى يتجاهلها الكثير من الناس. لذلك من الأفضل أن تقوم بتشغيل برنامج تحديث الويندوز أسبوعياً وكلما وجهت مايكروسوفت تحذير. وسيظل على المستخدم القيام بنفسه بالتحديث إلى أن يتم عمل برنامج تحديث تلقائي .

7 لا تنسي عمل Rescue disk

عندما يضطرب النظام لديك فإن Rescue disk أفضل حل أو على أقل تقدير ستحتاج إلى أن تضع العناصر الأساسية لنظام التشغيل على قرص من floppy disk أو Zip media حتى تتجنب القرص الصلب أثناء الدخول . ومن الأفضل أن تستخدم البرنامج المضاد للفيروسات الخاص بك لعمل Rescue disk تستخدمه عند إصابة النظام. أكتب عليه تاريخ أنشاؤه واحتفظ به لحين الحاجة .

8 لا تنخدع بالإنذارات الكاذبة

توجد وسائل خداع أشد من الهاكرز على الإنترنت فكثير من الإنذارات الكاذبة عن فيروسات الإيميل أكثر من الفيروسات الحقيقية . حتى التحذيرات العادية من الفيروسات تأخذ أكثر من حجمها الطبيعي إعلامياً .

وقد تتسبب الإنذارات المزيفة بإلغاء ملفات غير ضارة و إرسال الرسالة للآخرين وتعطيل خدمات الإيميل وتتسبب في أضرار "شبه فيروسيه". لذا عندما تصلك إحدي تلك الرسائل أو خبراً تحذيري تأكد أولاً. أكتب إسم الفيروس المزعوم في محرك بحث لترى إذا كان هناك بالفعل تحذير منه، ويمكنك أيضاً زيارة مواقع الفيروسات المزيفة .

9 لا تتجاهل أهمية الـ Firewall

إن برنامج الـ Firewall تعمل فى الكمبيوتر وكأنها منظم لحركة الدخول والخروج فهي تفحص كل البيانات قبل دخولها ولا تسمح لأي بيانات بالدخول أو الخروج إلا إذا كنت تسمح أنت . لذلك لن يستطيع الهاكر كشف بياناتك الشخصية على جهازك ولا تستطيع برامج مثل Trojan horse keystroke logger أن تسرق كلمة السر الخاصة بك وإرسالها عبر الإنترنت. فهناك برامج Fire wall كفيلة بصدها، ولكن الحل الأمثل هو برنامج واحد يشمل مضاد الفيروسات والسبام والنوافذ التلقائية الفتح والـ Fire wall أيضاً .

10 لا تنسى إنشاء ملفات احتياطية Back up

انشئ بيانات احتياطية لبياناتك بشكل أسبوعي (ويومياً إذا كنت صاحب عمل) فحتى لو وقعت ضحية لفيروس أو هاكر ، فستكون الأضرار بسيطة ولكن إذا فشلت فى الاحتفاظ بملفات احتياطية ستعاني كثيراً إذا أتلفت ملفاتك الهامة.